ELECTRONIC TENDER SYSTEM

BACKGROUND OF THE INVENTION

[0001] The present invention relates to an electronic tender system, and particularly to a method for coding a bid and a method for deciding a contract price.

[0002] As known from Japanese Patent Laid-Open No. HEI2-118876, for example, an electronic tender system uses coding technology because the bid information should be kept confidential until the tender opening. All coded bid information is decoded at the tender opening to decide the highest or the lowest bid as the contract price. The announcement of all bids allows all bidders to confirm that the contact price has been decided correctly, in other words, it was the highest or the lowest price among the bids.

[0003] Recently, it has become important not to publish the unaccepted bids because of privacy concerns. To meet this requirement, for example, an approach has been disclosed in an article, "Multi-round Anonymous Auction Protocols" by Kikuchi, Harkavy and Tyger, published. in "IEEE Workshop on Dependable and Real-time E-Commerce System". This approach disclosed in the prior art literature is shown in Fig. 1.

[0004] In this approach, the bidder creates a data row corresponding to a series indicating bids at successive bid prices. If the bidder wishes to offer a bid at a given price, the bidder's ID is supplied in correspondence to that price. If the bidder does not wish to offer a bid at a given price, a value 0 is supplied in correspondence to that price. This series of data forms a data row. Each data row is encoded. The opener receives encoded data rows transmitted by all bidders, adds them together and then decodes the sum to determine the contract price. In this approach, as the code string data of individual bidder is not decoded, the bid of respective bidder can be kept secret, and at the same time, the identification information of the highest price bidder can be extracted from the sum of the data rows.

[0005] Now, the principle of identification extraction will be described. A bidder having an identification information IDi, creates a data row corresponding

to his bids as follows. Suppose the tender reception range be (a, b) and his bid a + v (<b), then (v + 1) times the bidder's ID are concatenated. This indicates that the bidder is willing to bid at each corresponding amount. Next, the value 0 is concatenated b - (a + v) times. This indicates that the bidder is not willing to bid at any of the corresponding amounts. Thus, a data row containing (b - a + 1) elements is generated.

[0006] A data row is then created from each received data row, in which the respective elements of each received data row are added. In the resulting data row, if the element where 0 appears first is labeled as the t^{th} element, the highest bid (contract price) is the bid corresponding to the a + t -1 element, and the winning bidder has identification information in that bidder's data row for the bid corresponding to the t - 1st element.

[0007] However, in this prior art, the bid data becomes longer in proportion to the tender reception price range, because the data row is created in proportion to the length of the tender reception range, and then it is divided to code. Further, when a plurality of bidders have offered the contract price, it is impossible to determine the identification or the number of concerned bidders, because the IDs of the winning bidders have been added together.

SUMMARY OF THE INVENTION

[0008] It is therefore an object of the present invention to provide an electronic tender system that reduces the amount of bid data, and at the same time, that identifies the winning bidders even when a plurality of bidders have offered the contract price, and moreover, to maintain the confidentiality of bid information for bids other than those of the successful bidders.

[0009] Other objects of the present invention will become clear as the description proceeds.

[0010] The electronic tender system according to the present invention is characterized in that a code parameter corresponding to a bid is delivered to a coding function section of a bidder sub-system. A contract price candidate selection function selects a candidate price, and a retrieve function retrieves a decode parameter corresponding to the candidate price that is used to determine

whether the candidate contract price is matched in a tender opening section. The use of code parameters and decode parameters that correspond to candidate contract prices allows a bid price to be known only if the bid is identical to a contract price candidate. Therefore, the highest or the lowest bid and its bidder can be determined by examining in sequence whether there is a bid identical to a contract price candidate and incrementing or decrementing the contract price candidate with respect to the possible highest price or the lowest price. Bids submitted by other bidders can be concealed in this manner.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Fig. 1 is a block diagram showing a conventional method;

[0012] Fig. 2 is a block diagram showing a composition of the present invention; and

[0013] Fig. 3 is a block diagram showing a composition of the retrieve section of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] Referring now to Figs. 2 and 3, description will proceed to an electronic tender system according to a preferred embodiment of the present invention.

[0015] Fig. 2 is a block diagram showing an embodiment of the present invention. The electronic tender system according to the present invention comprises a bidder sub-system 100 and a tender opening sub-system 200. The bidder sub-system 100 includes a code parameter acquisition section 101 and a coding section 102, while the tender opening sub-system 200 includes a reception section 201, a contract price candidate selection section 202, a decode parameter acquisition section 203 and a retrieve section 204.

[0016] The retrieve section 204 includes, as shown in Fig. 3, a decoding section 205 and a judgment section 206. The decoding section 205 sequentially decodes coded bids received by the reception section 201 using a decode parameter corresponding to a candidate bid that is acquired by the decode parameter acquisition section 205. The judgment section 206

determines that a decoded bid is identical to the contact price candidate selected by the selection section 202 when the decoding result produced by the decoding section 205 is a predetermined value.

[0017] Note that, in this embodiment, to simplify the description, it is supposed, hereinafter, that a bidder subsystem that has offered the highest price, among bid prices, will be decided as the successful bidder, though it is similar in the case where the lowest price will be the successful bid that determines the contract price.

[0018] The input to the bidder sub-system 100 is the bid desired by the bidder sub-system. The bid by this bidder sub-system 100 is delivered to the code parameter acquisition section 101. In the code parameter acquisition section 101, a code parameter that is used by the coding section 102 and that corresponds to the amount of this bid is acquired and delivered to the coding section 102. The coding section 102 performs the coding operation based on the supplied code parameter, and delivers the coded bidding data to the transmission section 103. The transmission section 103 transmits the coded bidding data to the reception section 201 of the tender opening sub-system 200.

[0019] The reception section 201 of the tender opening subsystem 200 receives the coded bidding data sent from bidder sub-system 100 and directs the contract price selection section 202 to begin a tender opening process on the tender opening day. The contract price selection section 202 directed to open the tender first takes the highest price within the acceptable range as a candidate price, and supplies the decode parameter acquisition section 203 with the candidate price.

[0020] The decode parameter acquisition section 203 acquires the decode parameter corresponding to the candidate price and delivers the decode parameter to the retrieve section 204. The retrieve section 204 decodes all coded bidding data received using the supplied decode parameter in the decoding section 205, and the judgment section 206 determines whether there is any bid among the coded bidding data that is the same as the candidate price. If a matching bid is determined, the bid of the bidder sub-system that sent the

corresponding coded bidding data will be accepted. If there is no coded bidding data having the candidate price as its bid, the retrieve section 204 outputs that the candidate price is not the contract price to the contract price selection section 202.

[0021] Upon the reception of this output from the retrieve section 204, the contract price selection section 202 takes the next lower price than the current candidate price as a new candidate price, and delivers the new candidate price to the decode parameter acquisition section 203. Then, operations as previously described will be repeated until the judging section 206 detects a successful bidder, or the candidate price becomes lower than the tender range. If the candidate price becomes lower than the tender range, it is judged that no bid is accepted, and this result is output before terminating the processing.

[0022] Now, as an example of this embodiment, the case where an El Gamal code is used as a coding function will be described. Since the El Gamal code is well known by those skilled in the art and is incidental to the present invention, its detailed explanation will be omitted.

[0023] First, the tender opening system creates a large prime p and a generator g. In addition, a secret key x (v), a public key y (v) and a constant M (v) for a respective bid v are decided. Here, the secret key x (v) and the public key y (v) present the following relation. M (v) may be an arbitrary value, and for example, v and its hash value can be linked as M (v), or may be a constant independent of v. As code parameters, M (v) and y (v) are adopted as code parameters and x(v) is adopted as a decode parameter. The code parameters are published, while the decode parameters are kept confidential in the tender opening sub-system.

[0024] The bidder sub-system 100 obtains the code parameters M (v) and y (v) that correspond to a bid v to be made, and codes M (v) with the public key y (v) based on the El Gamal code. The El Gamal code, belonging to the code type called probabilistic encryption, is known to produce a different coded message even if the same M (v) is coded. The bidder sub-system 100 sends this coding result to the tender opening system 200 as coded bidding data C (v).

[0025] The tender opening sub-system 200 obtains a decode parameter x (v') for a contract price candidate v' and decodes C (v) using this decode parameter as the secret key. If v = v' obviously the decoding result will be M(v) = M (v'). On the contrary, if v v', the decoding result will not be M(v'). Thus, without revealing the bid, it can be determined whether the bid is equal to the contract price candidate.

[0026] If the contract price is decided to be v, all offered code bids, and the decode parameter x (v) corresponding the possible bidding prices that are equal to or larger than v are published by the announcement section. Therefore, all bidders can verify that there was no bid larger than v and can determine who has bid the contract price, since each bidder can attempt to decode all offered coded bids using the announced decode parameter.

[0027] On the other hand, bids inferior to the contract price can be concealed, as the decode parameters x (v) corresponding to the bids that are less than the contract price are not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding subsystems have offered the contract price.

[0028] As another specific embodiment, a case where RSA code is used for coding function will be described. The detailed description of the RSA code will be omitted as it is well known by those skilled in the art and is incidental to the present invention. For RSA coding, a code parameter y (v) is generated automatically from the bid v, without table lookup, and moreover, the fixed value M (v) to be coded may not be fixed for all bidders.

[0029] First, the tender opening system generates large primes p and q, and determines their product n. The bidder sub-system generates the code parameter M (v), y (v), for the bid v it wishes to offer. That is to say, it generates random numbers, and makes M (v) be the concatenation of v, and this random number, and the hash value where they are coupled. Next, y (v), 1 is concatenated with the hash value of v, making it prime to (p-1)(q-1).

[0030] Then, M (v) is codified with the public key y (v) based on the RSA code of the modulus n. In this case, as different random numbers are generated

for respective bidders, different coded messages are generated even if a same v is coded. The bidder sub-system transmits this coding result to the tender opening system 200 as coded bidding data C (v).

[0031] The tender opening system 200 calculates y (v') corresponding to a contract price candidate v', namely its hash value, and calculates x (v') that is the inverse element of y (v') in the modulus (p- 1)(q-1), as a decode parameter. Then, C (v) is decoded in the modulus n taking this code parameter as the secret key.

[0032] Here, if v = v', the decoding result M (v') will have a correct format for v' and a certain random number. On the other hand, if v v', the decoding result will not have such format. Thus, without revealing the bid itself, it can be determined whether the bid is equal to the contract price candidate.

[0033] If the contract price is decided to be v, all offered code bids, and respective result of decoding by the decode parameter x (v) corresponding the possible tender prices that are equal to or larger than v are published by the announcement section. Therefore, all bidders can verify that there was no bid larger than v and identify the successful bidder, since they can confirm that the result coded by the code parameter y (v') corresponding to the contact price candidate is equal to the offered coded bids using the announced decode parameter.

[0034] On the other hand, bids inferior to the contract price can be concealed, because the decoding result corresponding to the bids that are less than the contract price are not published. Further, problems in the case where a plurality of successful bidders exist as in the conventional method will not occur, because all bidding sub-systems will be identified, even when obviously a plurality of bidding subsystems have offered the contract price.

[0035] Moreover, it is assured that coded bids to be input into the tender opening system exclude those outside the bidding period, by publishing coded bids that are received before the bidding deadline, and opening only the published bids. As this is incidental to the present invention, further detailed description of this feature will be omitted.

[0036] Additionally, it can be assured that the tender opening system will not illegally decode the coded bid, such as by controlling or generating different decode parameters using a plurality of sub-systems that employ a distributed secret or group decryption technology or the like. As this feature is also incidental to the present invention, further detailed description will be omitted.

[0037] In addition, a digital signature may be used with a coded bid in order to prevent the bidder from bidding in the name of another bidder, or denying responsibility for a transmitted coded bid; however, this feature is also incidental to the present invention, so further detailed description thereof will be omitted.

[0038] In the disclosed embodiment, the case where a bidding sub-system that has offered the highest price among bid prices is the successful bidder has been described in detail; however, similarly, the invention may also be applied to the case wherein the lowest price will be the contract price, or to the case wherein a plurality of bidding sub-systems that have offered a bid close to the highest price or the lowest price are treated as winning bidders.

[0039] It is to be understood that the present invention is not limited to the aforementioned respective embodiments, and obviously, the respective embodiments can be executed by conveniently modifying them, without departing from the technical concept of the present invention.

[0040] As described hereinbefore, according to the present invention, it is possible to provide an electronic tender system that selects the bidder who has offered the highest or the lowest price as successful bidder, and moreover, that maintains the confidentiality of bidding information for bids other than those of the successful bidders, based on a basic composition wherein bidder sub-systems code their bids by means of a code parameter that corresponds to a particular bid value, and the tender opening system decodes by a decode parameter that corresponds to a particular contract price candidate.